

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
1 November 2001 (01.11.2001)

PCT

(10) International Publication Number
WO 01/82092 A1

(51) International Patent Classification⁷: **G06F 15/00** (74) Agent: FREEHILLS CARTER SMITH BEADLE; 101 Collins Street, Melbourne, VIC 3000 (AU).

(21) International Application Number: PCT/AU01/00451

(22) International Filing Date: 19 April 2001 (19.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PQ 7042 20 April 2000 (20.04.2000) AU
PQ 7974 6 June 2000 (06.06.2000) AU

(71) Applicant (for all designated States except US): AUSTRALIA AND NEW ZEALAND BANKING GROUP LIMITED [AU/AU]; 100 Queen Street, Melbourne, VIC 3000 (AU).

(72) Inventor; and

(75) Inventor/Applicant (for US only): DANKS, David, Hilton [AU/AU]; c/- Level 20, 570 Bourke Street, Melbourne, VIC 3000 (AU).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

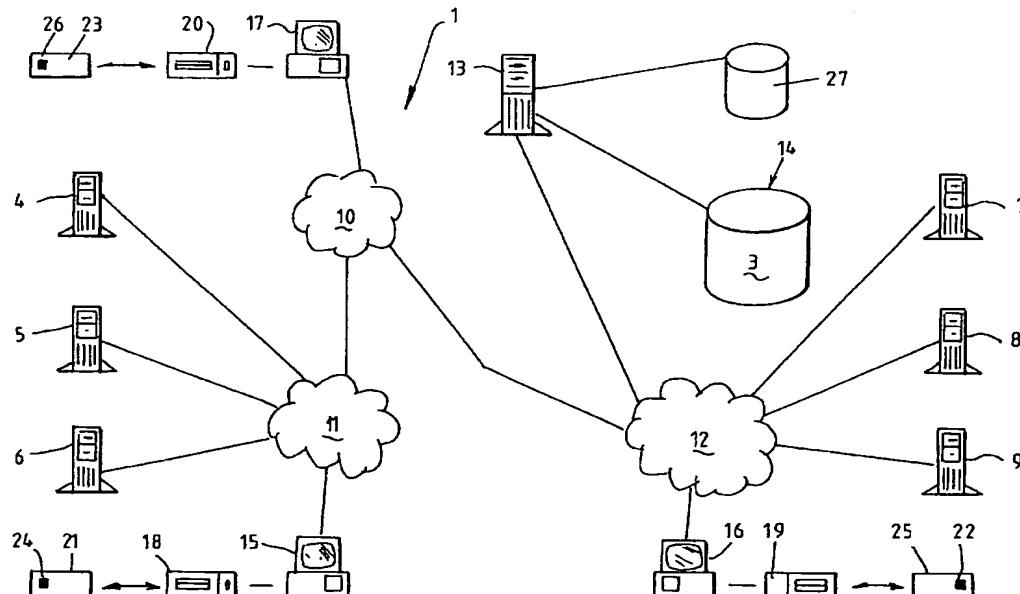
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE SYSTEM ACCESS



WO 01/82092 A1

(57) Abstract: A method of managing access to secure resources (4-9), the method including: providing an schema of permission rights in respect of secure resources; and, delegating to one or more users an ability to delegate (32) a profile (31) of selected permission rights in respect of one or more secure resources.

- 1 -

SECURE SYSTEM ACCESS

The invention relates to system access, and relates particularly though not exclusively to the management of secure environments for e-commerce

5 systems.

The Internet, and more particularly the World Wide Web, has created new opportunities for conducting commercial transactions electronically. In this respect, electronic commerce between businesses (B2B e-commerce) is expected to become ever more pervasive. Accordingly, the ability of vendors to

10 manage the process of identifying users and granting those users access to a vendor's Web site is increasingly problematic. Without an adequate system, a vendor cannot appropriately control who is permitted access to its systems. This risk exposure can potentially result in inappropriate system usage.

Existing access methods allow the user to access their vendor's secure

15 Web site or network and conduct business electronically (such as over the Internet) through network to network connections. A user attempting to access a particular site for the purpose of a transaction must have corresponding software installed on their computer. An initial set up procedure is required for each new user of the software before they are granted permission to access the

20 vendor's network.

This technique is relatively labour intensive. As a result, many of the efficiencies that might otherwise be achieved as a result of doing business electronically can be negated, due in large part to the inconvenience associated with system management.

25 Another approach is to link up the computer networks of two parties to facilitate e-commerce transactions. This can also be a costly and time-consuming practice, as external consultants are generally needed to facilitate such a connection, and significant costs are incurred from the increased labour and the need to purchase new software and hardware. Such methods are also

30 unsuitable for B2C e-commerce due to the costs and expertise required. This approach also poses significant security risks for both parties in the event of one

- 2 -

end of the system becoming compromised, or the business relationship between the two parties becoming hostile. The ability of one party to cause damage to the other's systems is a tangible risk exposure for both parties.

5 In short, current methods are generally deficient as they involve a reasonably high amount of negotiation between parties, with consequent costs. Accordingly, it would be desirable to address these and other problems associated with existing systems and techniques relating to the administration of permission rights.

10 The Applicant has recognised that access to secure resources can be advantageously administered by allowing for the delegation of permission rights to one or more users who, in turn, are also able to delegate permission rights to other users. It is recognised that decentralised administration of permission rights can be advantageously combined with a centralised administration of the execution of those rights.

15 One aspect of the invention provides a method of managing access to secure resources, the method including:

providing an schema of permission rights in respect of secure resources; and,

20 delegating to one or more users an ability to delegate a profile of selected permission rights in respect of one or more secure resources.

Each of said profiles of permission rights may be centrally maintained in a central server. Moreover, one or more of the secure resources may be hosted remotely from the central server

25 Preferably, the schema of permission rights is a logical arrangement of different permission rights that have an implied hierachial order. Preferably, the schema is extendable to allow the grant of permissions in relation to the secure resources. Preferably, the secure resources are either information sources or applications.

30 Preferably, at least a first of the users is able to delegate to another user a profile of selected permission rights which is less than or equal to the permission rights held by the first user.

- 3 -

Preferably, said central server grants or denies requests made by users in respect of said secure resources. Preferably, activities of users are centrally audited and tracked in the central server. Preferably, requests to the central server are referred by servers that receive requests from remote users.

5 Preferably, each of said profiles of permission rights represent a profile in respect of a particular set of one or more secure resources.

Preferably, said permission rights govern access to generally restricted information, or use of generally restricted functionality. Preferably, said secure resources are information-based or functionality-based resources, access to 10 which is generally restricted subject to verification of access rights is respect of said resources.

Preferably, there is for each user and each secure resource an associated access right. That is, there is for each secure resource a set of access rights associated with respective users.

15 The Applicant has recognised that a neutral provider can advantageously act as a central hub for the administration of access rights to sensitive information stored on the servers of various organisations.

Another aspect of the invention provides a method of allowing secure access to a remote system via a network, the method including:

20 (a) storing in a central server a database of permission rights for a plurality of secure resources stored in one or more remote servers;

(b) receiving a request for access to one of said respective secure resources from said plurality of remote servers;

(c) establishing the identity of a user making said access request;

25 (d) determining whether the user has permission rights which are sufficient to allow the user to access said one secure resource; and

(e) approving or declining said access request if the permission rights of the user are or are not sufficient to allow the user to access said one secure resource.

30 Preferably, said request is made to one of said remote servers and is redirected from that remote server to said central server.

- 4 -

A further aspect of the invention provides a method of allowing secure access to a remote system via a network, the method including:

- (a) receiving a request for access to a secure resource;
- (b) establishing the identity of a user making said access request;
- 5 (c) determining whether the user has permission rights which are sufficient to allow the user to access the secure resource; and
- (d) approving or declining said access request if the permission rights of the user are or are not sufficient to allow the user to access the secure resource;

10 wherein the secure resource is stored at a remote server, and requests for access to the secure resource are received at the remote server and redirected to a central server.

15 Preferably, upon approval of the access request, a second remote server directs the access request to a first remote server, and the first remote server responds to the user.

20 Preferably, establishing the identity of the user involves the use of identification codes such as, for example, digital certificates. Preferably the digital certifications use public key cryptography techniques. Preferably, one or more users with appropriate permission rights can issue their identification codes for other users. Preferably, those one or more users can specify the permission rights enjoyed by the other users for whom they issue identification codes.

25 Preferably, the secure resources are formatted in a manner specific to the user making the access request.

30 The described methods can be used to facilitate electronic commerce transactions, by allowing organisations to administer and establish their own hierarchy of permission rights for a number of users. Preferably, a software tool or wizard is provided for allowing the organisation to develop and manage these permission rights.

35 Preferably, users can be delegated the capability to issue digital identification certificates, including Identrus certificates, to other users.

Preferably, the secure server is capable of operating at a remote site and using digital certificates stored on a smart card to verify the permission rights of a third party.

In particular embodiments, it is preferred that a software application or 5 component (such as, for example, a Java applet) can be downloaded onto a user's computer for the purpose of encoding a smart card with a public key and a private key. Permission rights are managed by an administrator with the appropriate permission level to grant appropriate access rights to users' smart cards.

10 The following description refers in more detail to the various features of the present invention. To facilitate an understanding of the invention, reference is made in the description to the accompanying drawings where the invention is illustrated in a preferred, but not limiting, embodiment.

In the drawings:

15 Fig. 1 is a schematic diagram of a system implementing the functionality of an embodiment of the invention;

Fig. 2 is a schematic diagram illustrating hierarchically ordered schemas of permission rights administered in the system of Fig. 1; and

20 Figs. 3 to 5 are flow diagrams illustrating the operation of various functionality of the system of Fig. 1.

Referring now to the drawings, a system 1 is provided in which a schema 2 of permission rights 3 is established to administer access to secure resources 4 to 9, such as particular resources (eg URLs) accessible from a computer network 10 to 12, and to which access is generally restricted.

25 The system 1 includes a central server 13 and a database 14 in which is stored, for each user, a profile of permission rights in relation to particular secure resources. These permission rights may be, for example, read/write/execute, or add/delete/modify/purchase or any other schema of permission rights that is appropriate. In this embodiment, the schema of 30 permission rights is fully extensive and can be adapted as required in relation to specific secure resources. For example, when a secure application is provided,

- 6 -

various application-specific actions can be defined, and corresponding permission rights established. As a result, it is possible to determine the level and type of access a user has to any of those application-specific actions.

When a new user is created, that user 30 is provided the ability to create a 5 further new user having a profile of permission rights that is at least equal to the profile of the creating user. Accordingly, new users are typically delegated:

- (a) a profile 31 of permission rights in relation to the secure resources, as well as
- (b) the ability to delegate 32 a profile of permission rights in relation 10 to those secure resources.

In some cases, an administrative user 33 will only be delegated the ability to delegate profiles of permission rights to other users, without any or only minimal permission rights of their own. In other cases, a particular user 34 will only be granted a profile of permission rights without the ability to delegate 15 profiles to other users.

The system 1 is intended to be used by organisations to allow any appropriate networked computing device to be used to add and delete users, and modify their permission and access / restriction levels and any other relevant criteria.

20 The system 1 allows authorised users, both internal and external to a particular organisation, to access secure resources or applications remotely from any computer or other access device, such as the terminals referenced 15 to 17 (for example, personal digital assistant). It is intended that each such computing device 15 to 17 is equipped with a smart card peripheral device 18 to 20 that is 25 able to read and write information from and to a smart card 21 to 23. The smart card stores a private key and public key pair 24 to 26 for identification of the respective smart card user. Preferably the system 1 uses digital certificates such as Identrus certificates, to authenticate users.

30 The computing device 15 to 17 can be positioned in any location that provides satisfactory network access. Accordingly, the computing device can be remote from the remaining infrastructure of the system, allowing for remote

- 7 -

distribution of the system. Computing devices using the system desirably have a smart card device for use with implementations which store certificates on smart cards.

The profiles of permission rights represented in Figure 2 are organised on 5 an application-by-application basis. Permission rights are granted on the basis of establishing a rule or "policy" for a particular action. Permission is only granted if a user has the appropriate attributes specified by the policy. If the user's permission profile does have appropriate attributes, header variables are passed to the application. These header variables contain name/value pairs 10 corresponding with the given user. This header variable information is used to build / customise the user interface that is presented to that user.

A policy for a given application specifies what types of users (ie profiles 15 of permission rights having particular attributes) can perform specified actions. Additionally, further information can be passed to the application, when and as required, to enable it to restrict the user's activity for any reason.

It should be noted that the attribute types such as view, maintain, drawdown, roll-over etc are all controlled by the application. The system's role 20 is to match the user with these attributes. The system does not process a user's attributes. The system merely passes information to particular applications specifying the user, and the permissions that user has. This may be, for example, viewing and drawdown only.

To provide a further explanation of the system, a particular example is now described. Initially, a user ID and password combination (or, alternatively, 25 a digital certificate) is stored on a hard drive of a particular computer or on a smart card 21 to 23. This forms the basis for identification. The system 1, however, is not implementation specific - various identification techniques can be incorporated into the system. Management of relationships and their permissions can be done from any computer as the smart card carries the digital certificate that provides the ID to the system, provided that the card has 30 sufficient authority to perform the action.

- 8 -

A company (ABC Pty Ltd) contacts the system provider (Central Authority) for the purpose of implementing the system for ABC Pty Ltd's Web site. The Central Authority identifies the user, possibly using the system to identify ABC Pty Ltd through an Identrus certificate that ABC Pty Ltd sends to 5 the Central Authority. All the security and access to the company's application is controlled and stored remotely on the Central Authority's server, including audit and non-repudiation functions.

ABC Pty Ltd then logs onto an online application form which is itself protected by the system. This application form allows ABC Pty Ltd access to 10 the system. This process can occur electronically, as indicated in Fig. 3. Accordingly, at step 50, the administrator access a wizard feature accessible from the central server 13 and fills in the position levels that a new employee is to have. At step 51, the central server 13 checks the administrator's ID and their permission levels to confirm that they have authority to set up the new smart 15 card with the specified access/permission levels. Permission is subsequently either denied at step 52 or, at step 53, the action is authorised. The administrator card is subsequently removed and the new employee smart card required to be encoded is inserted in the corresponding smart card reader at step 54. At step 55, the central server 13 provides data to the remote user terminal in 20 question to enable the encoding of the new smart card with the appropriate permission levels. At step 56, the administrator is then able to provide the new employee with their personal smart card. At step 57, the central server 13 then creates a new user within the particular company permissioning structure maintained in the database 14.

ABC Pty Ltd takes the system to their developers, who install the system 25 to the front end of ABC Pty Ltd's Web system. During this process, the URL hierarchy, the database structure, application administrators, information regarding which URLs are protected as a secure resource and the business rules within the URLs, are loaded onto the database through one or more software 30 "wizards" 27 or other tools.

The administrator (possibly the departmental heads) will build further screens for the users and set up the users with unique profiles of permission rights using other wizards. The users may be staff, or external customers. Each of the users are provided with a smart card (or a user ID and password combination) that will enable them to access certain restricted URLs of ABC Pty Ltd applications. Particular applications will allow certain users to create new profiles, and corresponding cards. The process of a user gaining access to secure resources is indicated in Fig. 4. A user logs onto ABC Pty Ltd's computer system. Requests for secure resources are intercepted at step 61 and 5 re-routed through the system. The system 13 determines at step 62 whether the user has sufficient and appropriate permission rights to access the secure resources. Depending on the outcome, the request is either denied at step 63 or 10 authorised at step 64.

As shown in Fig. 5, ABC Pty Ltd's customer (XYZ Pty Ltd) can take a 15 smart card, and log onto ABC Pty Ltd's Web site at step 70 from any computer, irrespective of location. If XYZ Pty Ltd try to access one of ABC Pty Ltd's restricted URLs, the system intercepts the request at step 71, challenges the user's ID at step 72, and check it off against the profile of permission rights stored in the system database for that user at step 73.

20 The Central Authority's server 13 completes the risk management activities at a site remote from those of the sites of remotely hosted secure resources 4 to 6 and locally hosted secure resources 7 to 9. The secure server 13 effectively acts as a hub through which permission-based request for access to 25 an organisation's secure resources must pass before permission to read/edit/delete etc the particular secure resource is granted or denied.

Each time a customer/staff member of a company wishes to access a secure resource 4 to 9 (such as, for example, a restricted access URL) to do something that requires a certain level of permission, an identification and authentication procedure is conducted.

30 The system 1 does not inherently limit the number of new users that can be issued permission rights. The system 1 also allows a first user to provide a

- 10 -

second user with a smart card or logon identification code which allows that second user access rights to the secure system which are equivalent to the first user. The system is safeguarded so that a first user cannot grant permission rights that are superior to those of the first user. Some exceptions to this general 5 rule exist. For example, in some cases, it is desirable that administrative personnel do not have permission rights to run some applications, but have the authority to create new users that do have such permission rights.

The administrator at XYZ Pty Ltd may initially wish to authorise users within XYZ Pty Ltd or within an allied company to access ABC Pty Ltd's Web 10 application. The process of doing this is analogous. The relevant personnel at XYZ Pty Ltd logs onto the system, which identifies and checks if they authorised to encode new cards for access to ABC Pty Ltd's application, and what level of permission rights they are authorised to allow on the issue of further cards.

15 ABC Pty Ltd can then market itself as having all its Web security protected by the Central Authority. The Central Authority thus effectively provides a risk management facility for ABC Pty Ltd. The system 1 also stores an audit and non-repudiation trail in the system database 14. Every B2B or B2C customer of ABC Pty Ltd can be assured that the privacy and security of their 20 information and transactions is protected by the Central Authority's risk management system, which is held remotely to ABC Pty Ltd.

ABC Pty Ltd is also assured that they can always identify a user 25 accessing secured resources on their Web site, and that user has been given access by one entitled to do so. ABC Pty Ltd can also be assured that they have non-repudiation of transactions undertaken through their Web site.

As the security access system 1 stores all relationships between users and permission rights, ABC Pty Ltd will also have the benefit of being able view a relationship tree displaying every user of their application and information on who authorised the access for that user. Reports of variable complexity and 30 type can be generated in relation to the various secure resources and users.

XYZ Pty Ltd also has access to view their branch of the ABC Pty Ltd permissioning tree. Administrators at both companies can manage and prune their relationship trees or branches as the need arises.

5 The privacy of the transmitted information is encrypted to ensure that it is secure on route to its destination. ABC Pty Ltd can also decide which parts of their application they wish to keep private from both internal and external customers.

10 The system 1 enables companies to allow users to access their application on a screen by screen basis. Each user can be given permission to access one particular URL and not another, and to perform one particular action at that URL and not another.

15 The system database 14 maintains records of the activities of developers and administrators for audit and non-repudiation purposes. This can be used to check the integrity of the application and for dispute resolution purposes.

20 15 A master wizard 27 can be used by the administrator at ABC Pty Ltd to sequentially build other wizards for master users to add, delete and determine the level of access new and existing users will have.

25 Access to a company's application can be from any computer 15 to 17. A session cookie 74 is downloaded onto the system for the duration of the session enabling access to the application.

30 The security system 1 described herein provides users with the ability to have all the administration of a permissioning system conducted at a remote and secure site, or secure server. The secure server 13 allows permissions 3 to be created and stored at its remote site.

25 The system 1 is particularly suitable for administering the security of a business organisation's data against abuse and inadvertent misuse by that organisation's staff, as all activities are able to be monitored by a trusted third party. The system 1 is particularly suitable for information-intensive organisations which deal in sensitive data which is required to be maintained and manipulated by a large number of staff on a regular basis for the same reason. Accordingly, the system 1 is particularly suitable for financial

- 12 -

institutions such as banks, or other data-based organisations such as hospitals, or insurance companies.

Terminals 15 to 17 used by the organisation to administer secure information include smart card readers 18 to 20 which are able to read the 5 contents of a smart card 22 to 24 used by relevant staff. The smart cards include a digital certificate 22 to 24 which identifies the respective staff member. The terminals and smart card readers may typically be within a single location, such as corporate headquarters, but may be just as easily be located through various offices, or off-site at, for example, a customer site. In short, terminals 10 interfacing with the central server can be located anywhere on a network typically the Internet 10, LAN 11 and 12, or a virtual private network.

In one implementation, a staff member swipes the smart card through the reader at the start of any session, and computer software executing on the computing device records the public and private keys for use during the session. 15 This computer software is preferably downloaded as required from the central server 13 and can thus be written, for example, as a Java® applet or application.

The system 1 enables the Central Authority to provide another business with the capability to use digital certificates (such as Identrus certificates) as a means of authenticating their users to other entities. This can be done remotely. 20 As an example, ABC Pty Ltd can use the system to verify their identity.

Once the system 1 has confirmed the identify to ABC Pty Ltd, a digital certificate can be issued using the system, which can then identify that user to another entity with which they may wish to deal, such as XYZ Pty Ltd.

The responsibility of who within ABC Pty Ltd can perform this function 25 rests with ABC Pty Ltd. The responsibility of the Central Authority is to be able to prove that the digital certificate was properly issued to an authorised user from the identified company, in this case ABC Pty Ltd. Effectively the Central Authority guarantees to XYZ Pty Ltd that ABC Pty Ltd is ABC Pty Ltd.

A further example of this process is to enable another organisation to 30 issue certificates as a means of identifying themselves and other individuals. For example, the Central Authority may wish to licence out the certificate

- 13 -

issuing process to another company once the Central Authority has checked their internal and external procedures. This proxy organisation can then issue certificates to third parties to allow those third parties to identify themselves when engaging in electronic transactions.

5 Once the encrypted keys have been presented to the application, a permission test is conducted at the secure server. The request is then either approved and re-routed to the requested Web site / network or transferred to an alternate Web page or screen advising that approval to enter that site was not given.

10 As described above, the system 1 includes the capability to allow any organisation to issue digital certificates through a standard Web browser or smart card. The system 1 includes the ability to allow individual smart cards to generate public and private key pairs through a smart card reader/writer . As described, these public and private keys form the basis of identification of users 15 for the administration of permission rights. It is preferred that permission attached to the first smart card issued to an organisation includes the capability to create further smart cards with varying permission profiles.

20 Thus the system 1 enables an organisation to manage and maintain its own permissioning structures 2. The encoding of each card issued by the organisation occurs at its discretion. The organisation will keep a track of the permissioning structure with the aid of software tool or wizard down to an individual level.

25 The system 1 also has the ability to customise the page depending on how a user wishes it to look. This information on how the smart card user wishes to view the page and what they view is also stored on the secure server and activated on initial logon. Upon gaining permission to view the site, the smart card communicates with the site and dictates how it should be viewed.

30 This feature enables the user to determine what information they need and makes the downloading of superfluous information unnecessary. This allows the browsing experience to be speeding up the process for the user.

- 14 -

The system 1 is designed to provide security and access to an organisation's applications. The system uses a variety of techniques to manage restricted access to these applications and resources.

It will be understood that the invention disclosed and defined in this
5 specification extends to all alternative combinations of two or more of the individual features mentioned or evident from the text or drawings. All of these different combinations constitute various alternative aspects of the invention.

- 15 -

CLAIMS:

1. A method of managing access to secure resources, the method including:
providing an schema of permission rights in respect of secure resources; and,
5 delegating to one or more users an ability to delegate a profile of selected
permission rights in respect of one or more secure resources.
- 10 2. A method according to claim 1, wherein each of the profiles of
permission rights is centrally maintained in a central server.
- 15 3. A method according to claim 2, wherein one or more of the secure
resources are hosted remotely from the central server.
- 20 4. A method according to any one of the preceding claims, wherein the
schema of permission rights is a logical arrangement of different permission
rights that have an implied hierachial order.
5. A method according to any one of the preceding claims, wherein the
schema is extendable to allow the grant of permissions in relation to the secure
20 resources.
- 25 6. A method according to any one of the preceding claims, wherein the
secure resources include information sources or applications.
7. A method according to any one of the preceding claims, wherein at least
a first of the users is able to delegate to another user a profile of selected
permission rights which is less than or equal to the permission rights held by the
first user.

- 16 -

8. A method according to any one of the preceding claims, wherein the central server acts to grants or denies requests made by the users in respect of said secure resources.
- 5 9. A method according to any one of the preceding claims, wherein activities of the users are centrally audited and tracked in the central server.
- 10 10. A method according to any one of the preceding claims, wherein requests to the central server are referred by servers that receive requests from remote users.
- 15 11. A method according to any one of the preceding claims, wherein each of said profiles of selected permission rights represents a profile in respect of a particular set of one or more secure resources.
- 20 12. A method according to any one of the preceding claims, wherein the permission rights govern access to generally restricted information or use of generally restricted functionality.
- 25 13. A method according to any one of the preceding claims, wherein the secure resources are information-based or functionality-based resources, access to which is generally restricted subject to verification of access rights in respect of said resources.
- 30 14. A method of allowing a secure access to a remote system via a network, the method including:
 - (a) storing in a central server a database of permission rights for a plurality of secure resources hosted at one or more remote servers;
 - (b) receiving an access request for access to one of the secure resources from one of the plurality of remote servers;
 - (c) establishing the identity of a user making the access request;

- 17 -

- (d) determining whether the user has permission rights which are sufficient to allow the user to access the one secure resource; and
- (e) approving or declining the access request if the permission rights of the user are or are not sufficient to allow the user to access the one secure

5 resource.

15. A method according to claim 14, wherein the request is made to one of the remote servers and is redirected from that remote server to the central server.

10 16. A method of allowing secure access to a remote system via a network, the method including:

- (a) receiving a request for access to a secure resource;
- (b) establishing the identity of a user making said access request;
- (c) determining whether the user has permission rights which are

15 sufficient to allow the user to access the secure resource; and

- (d) approving or declining said access request if the permission rights of the user are or are not sufficient to allow the user to access the secure resource;

wherein the secure resource is hosted at a remote server, and requests for

20 access to the secure resource are received at the remote server and redirected to a central server.

17. A method according to claim 16 wherein, upon approval of the access request, a second remote server directs the access request to a first remote

25 server, and the first remote server responds to the user.

18. A method according to either one of claims 16 or 17, wherein establishing the identity of the user involves the use of identification codes.

30 19. A method according to claim 18, wherein the identification codes comprise digital certificates.

20. A method according to claim 19, wherein the digital certifications use public key cryptography techniques.

5 21. A method according to any one of claims 16 to 20, wherein one or more of the users with appropriate permission rights can issue identification codes for other users.

10 22. A method according to claim 21, wherein said one or more of the users can specify the permission rights of the other users to whom identification codes are issued.

15 23. A method according to any one of claims 16 to 22, wherein the secure resources are formatted in a manner specific to the user making the access request.

20 24. A method according to any one of the preceding claims, and further including using a software tool or wizard to develop and manage the permission rights.

25. A method according to any one of the preceding claims, and further including delegating to one or more of the users the capability to issue digital identification certificates to other users.

25 26. A method according to claim 25, wherein the digital identification certificates include Identrus certificates.

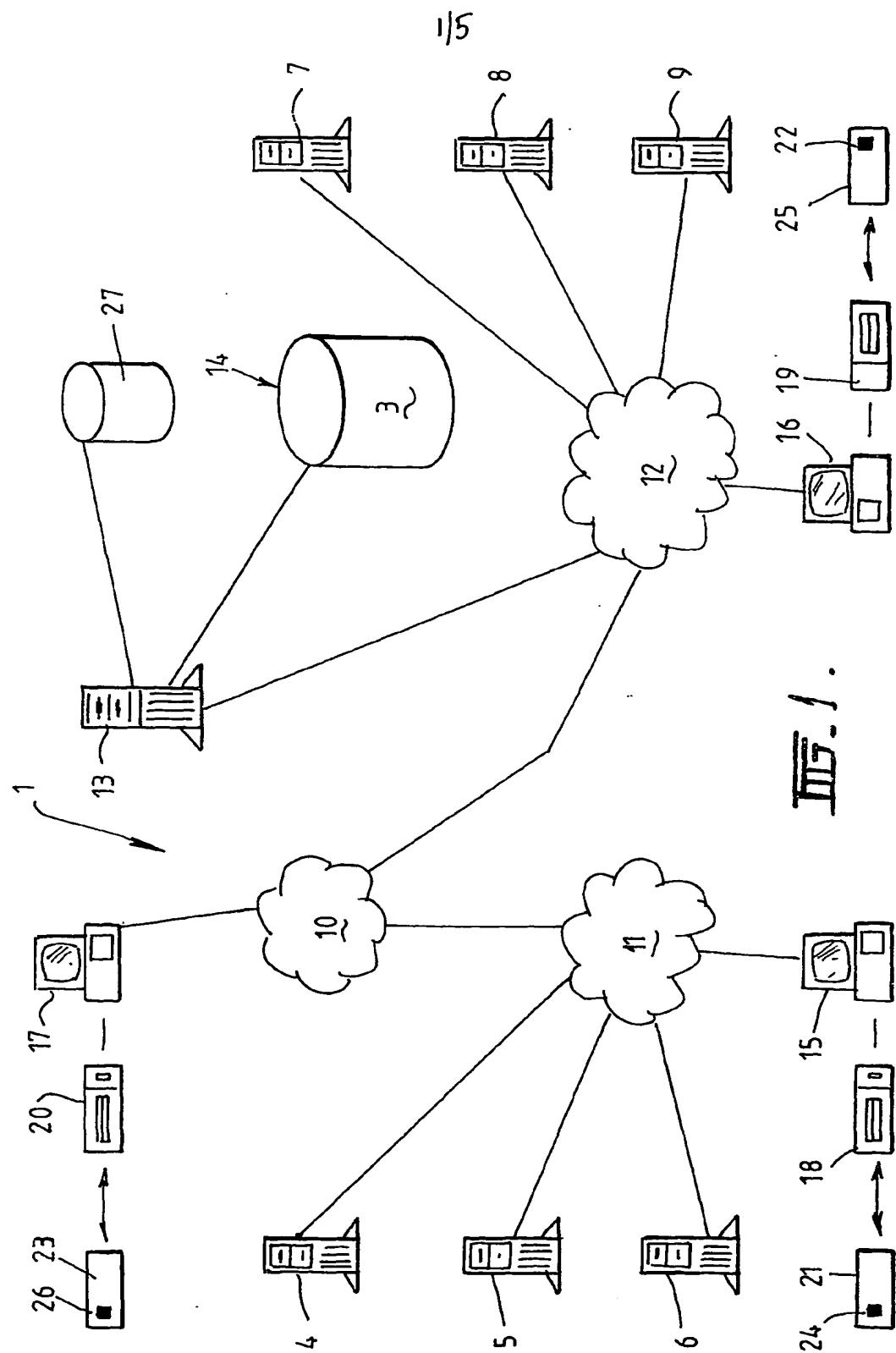
30 27. A method according to either one of claims 25 or 26, wherein the secure server operates at a remote site and uses the digital certificates stored on a smart card to verify the permission rights of a third party.

- 19 -

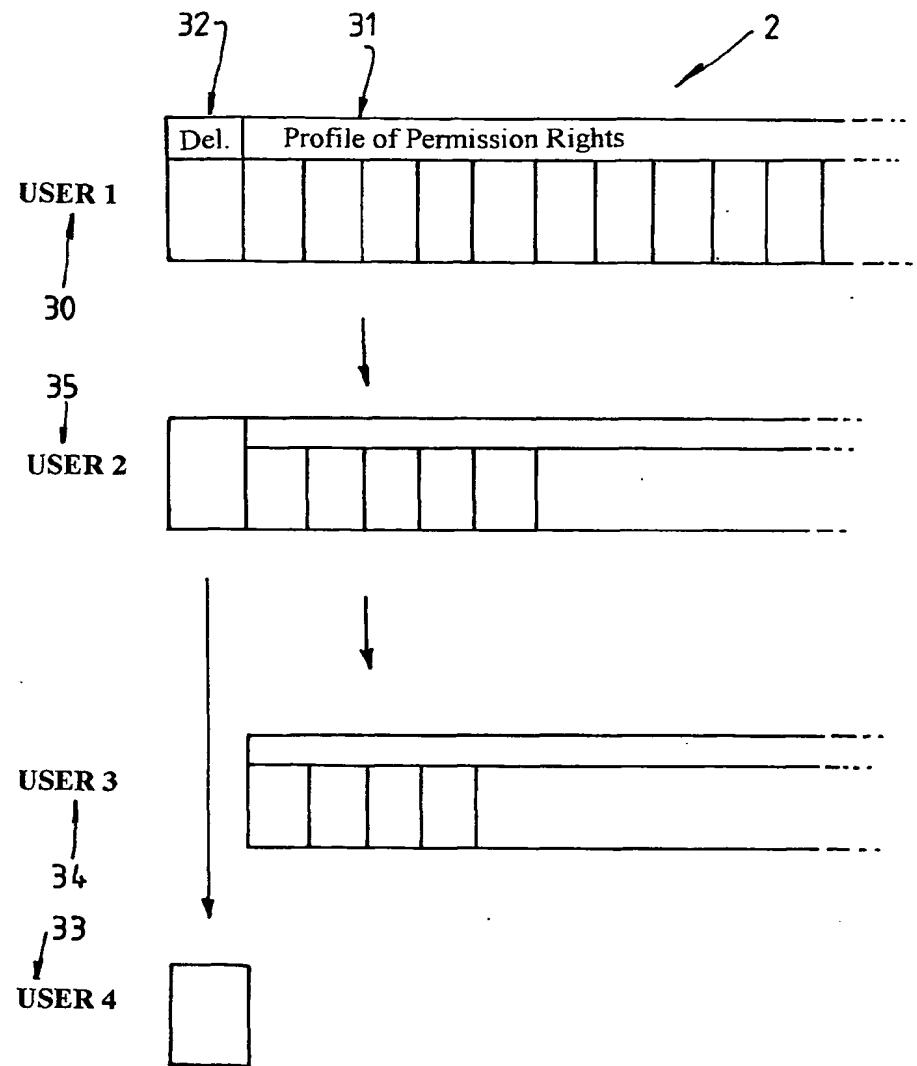
28. A method according to any one of the preceding claims, and further including downloading a software application or component onto a user's computer for the purpose of encoding a smart card with a public key and a private key.

5

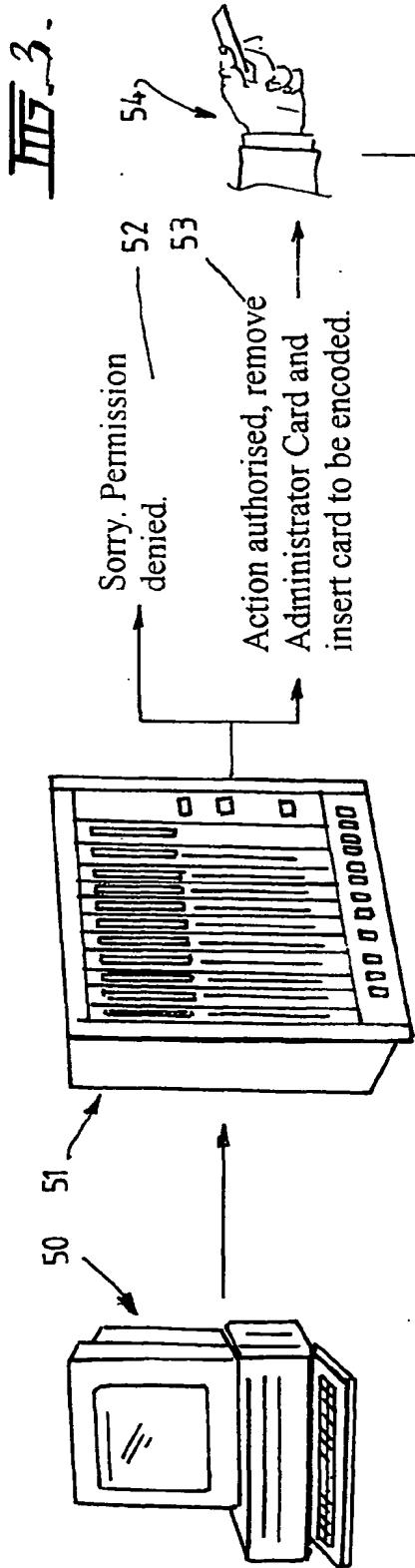
29. A method according to claim 28, wherein the permission rights are managed by an administrator with the appropriate permission level to grant appropriate access rights to users' smart cards.



2 | 5

III. 2.

3/5



SAM checks the Administrator's ID and their permission levels to confirm that they have the authority to set up the new card with the specified access/permission level.

50 51

52 53 54

55 56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

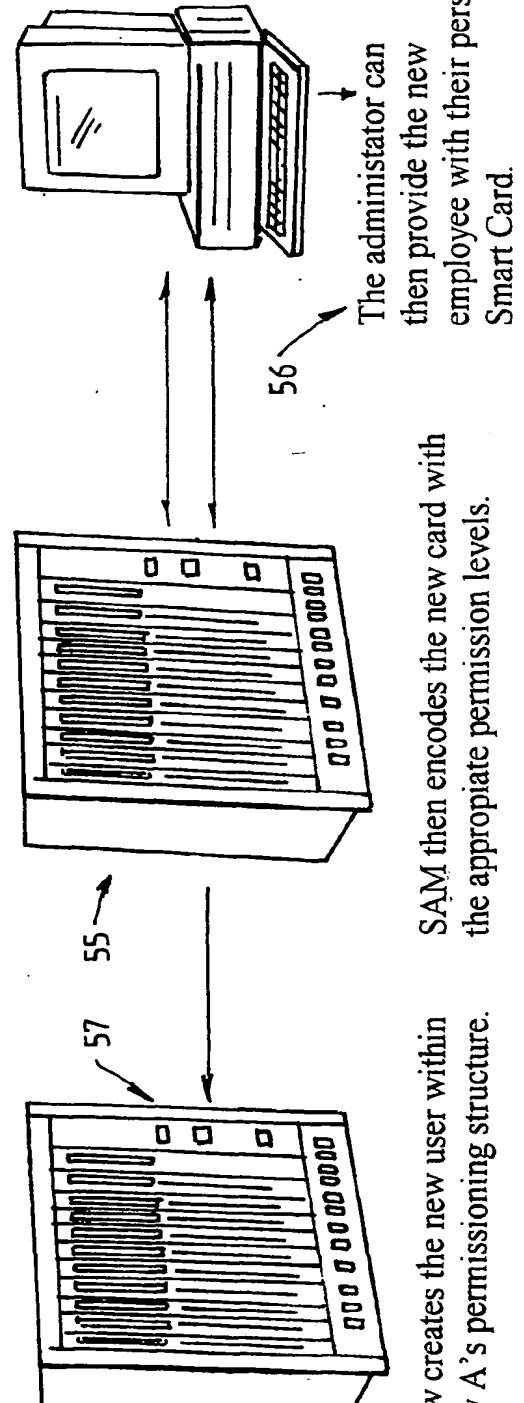
996

997

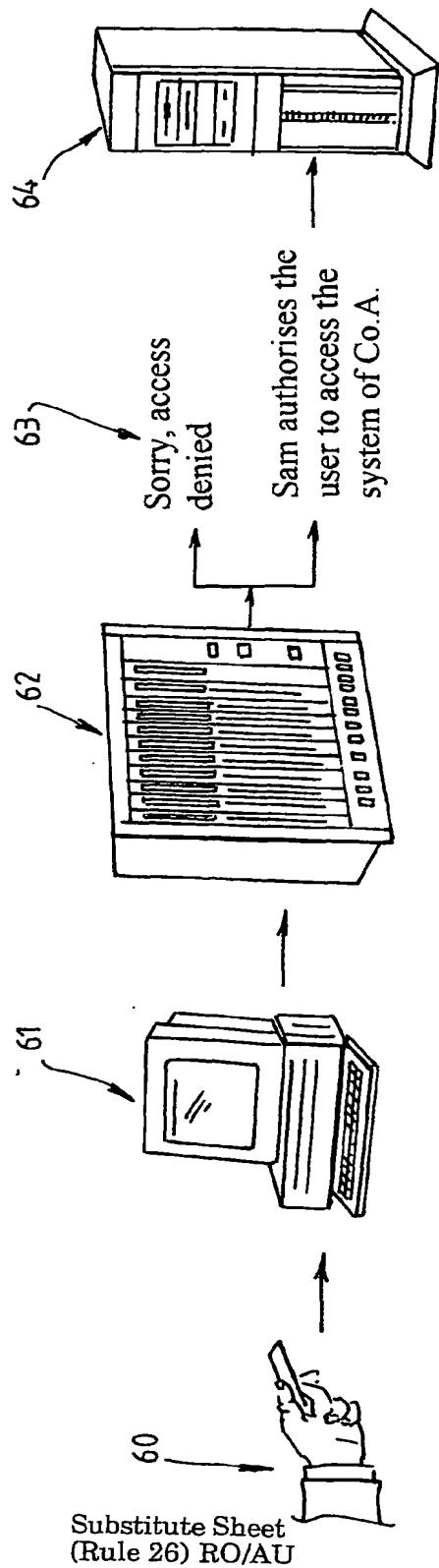
998

999

1000



4/5

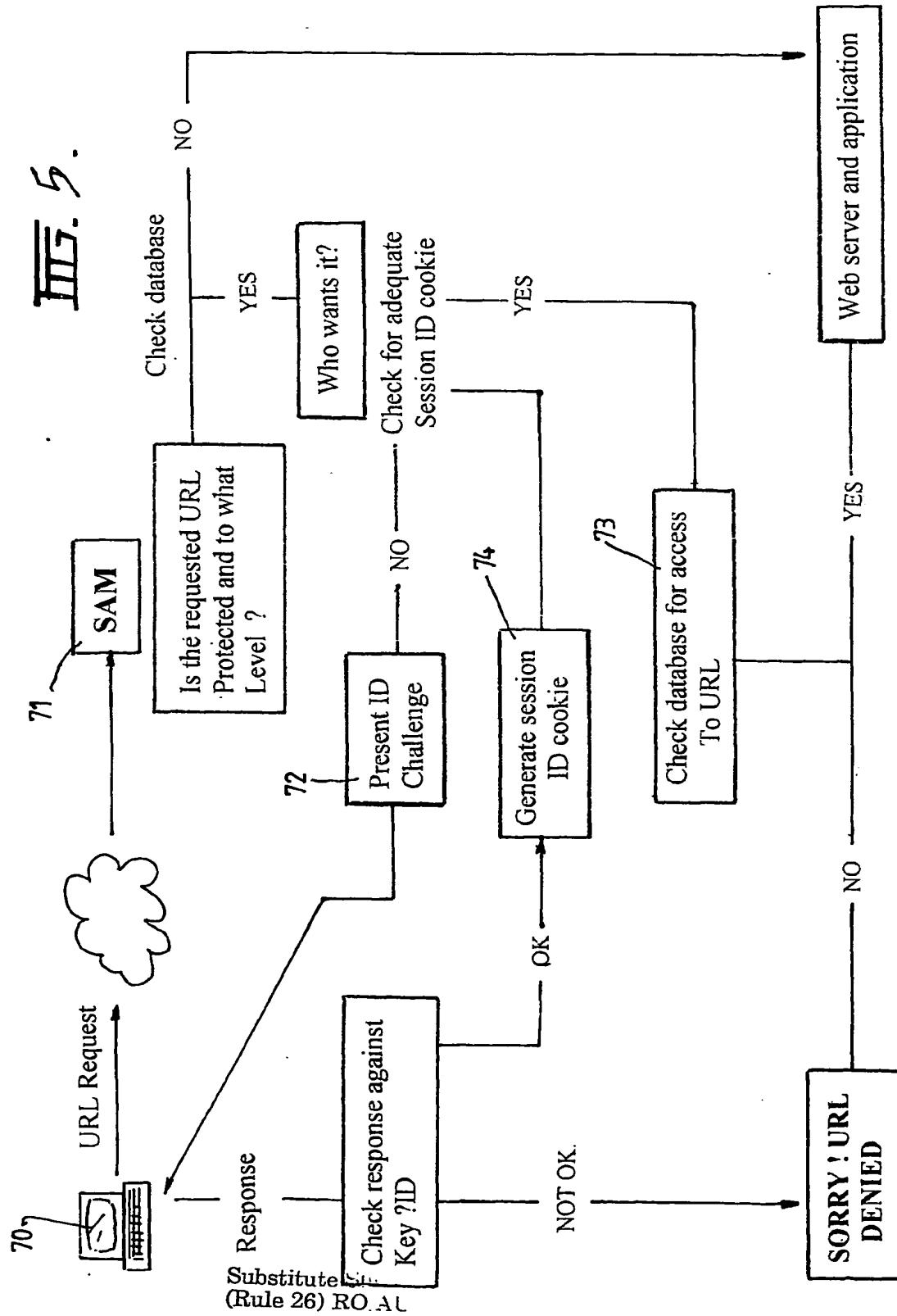


A staff member of Company A inserts their smart card into the reader of any computer and logs on to their company's system. This request is intercepted and re-routed to SAM

Sam confirms that the smart card of the employee has sufficient permission to access the system.

III. 4.

515



INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU01/00451

A. CLASSIFICATION OF SUBJECT MATTER		
Int. Cl. ?: G06F 15/00		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) WPAT, USPTO (KEYWORDS): NETWORK, INTERNET, SERVER, ADMINISTRAT+, PRIVILEG+, DELEGT+, HIERARCH+...		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98/40992 A (INTERNET DYNAMICS, INC) 17 September 1998 See whole document	1-29
X	EP 570683 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 24 November 1993 See whole document	14-29
A	US 5729734 A (PARKER et al) 17 March 1998 See whole document	
<input type="checkbox"/> Further documents are listed in the continuation of Box C <input checked="" type="checkbox"/> See patent family annex		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed		
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 18 July 2001		Date of mailing of the international search report 24 July 2001
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaaustralia.gov.au Facsimile No. (02) 6285 3929		Authorized officer Stephen Lee Telephone No : (02) 6283 2205

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU01/00451

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member			
WO	9840992	AU	64527/98	EP	966822
EP	570683	JP	6029993	US	5642515
US	5729734	NONE			
END OF ANNEX					